REMARKS

Claims 1-57 are pending in the present application. Claims 1, 27, 37 and 44 have been amended, and new claims 54-57 have been added.

Applicant respectfully responds to this Office Action.

Claim Rejections – 35 USC § 102(a)

Claims 1-53 were rejected under 35 U.S.C. §102(a) as being anticipated by Ekdahl et al., "SNOW – a new stream cipher", Nov. 2001 (hereinafter referred to as the Ekdahl publication).

The rejection of claim 1 as being anticipated by the Ekdahl publication is respectfully traversed. Claim 1, as amended, recites, "A method of generating a key stream comprising: applying a cryptographic function on at least five input values selected from a first array of values to generate at least five output values; selecting at least five mask values from a second array of values; and combining the at least five output values with the at least five mask values to generate a key stream block for the key stream; wherein the first and second arrays are finite." Support for the amendments to claim 1 is shown in Figure 6 by the exemplary input values A, B, C, D and E selected from an array of values in LFSR 610, and by the exemplary mask values A', B', C', D' and E' selected from a new or an updated array of values in LFSR 610. The Ekdahl publication fails to disclose a key stream block generated from combining at least five output values with at least five mask values. Instead, the SNOW generator of the Ekdahl publication produces a running key (Fig. 1), by bitwise adding the output of the finite state machine (FSM) with the last entry (32 bits) of the LFSR. The Ekdahl publication teaches combining only the last entry of the LFSR with the FSM output to generate the running key. Therefore, only one 32-bit entry or value of the LFSR's array of values is selected and combined in generating the running key. Thus, the Ekdahl publication fails to anticipate all of the features recited in amended claim 1. Accordingly, the rejection of claim 1 as being anticipated by the Ekdahl publication should be withdrawn.

It is respectfully submitted that dependent claims 2-26 are at least allowable for the reasons given above in relation to independent claim 1. Of particular note are claims 3-5 and 7, which associate the values of the first array with a LRSR. However, in the Office Action, with respect to claim 1, the Examiner associates the FSM with the first array of values, and then, with

respect to claims 3-5, the Examiner associates the LFSR with the first array. See, Office Action, pages 2-4. Thus, the rejections of claims 3-5 are inconsistent with the rejection of claim 1. Also, claim 10 recites that "the first and second arrays each comprises seventeen values". However, the FSM does not have seventeen registers, and the LFSR of the SNOW generator has only 16 registers.

Claims 27-53 are apparatus and computer readable medium claims having features defined by language similar to that of method claims 1-26. Claim 27 recites "means for combining the at least five output values with the at least five mask values to generate a key stream block for the key stream", claim 37 recites, "combining the at least five output values with the at least five mask values to generate a key stream block for the key stream", and claim 44 recites, "a combining module configured to combine the at least five output values with at least five mask values selected from a second array of values to generate a key stream block for the key stream". Accordingly, for the reasons recited above with respect to claims 1-26, claims 27-53 define patentable advances over the Ekdahl publication, and the rejections of claims 27-53 should be withdrawn.

New Claims

Support for new claims 54-57 may be located in Figures 2 and 6, and in original claims 5, 31, 39 and 48. Applicants respectfully asserts that new claims 54-57 recite patentable matter as discussed above with respect to claims 1-53, and for recitation of each input value, output value, and mask value comprising one or more words, each word having two or more bytes, and the key stream block comprising five or more words, each word having two or more bytes.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicant submits that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: **August 21, 2008**

By: /Won Tae C. Kim /
Won Tae C. Kim, Reg. # 40,457
(858) 651 - 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502